STATEMENT

John N. McMahon, Deputy Director of Central Intelligence

Senate Select Committee on Intelligence Hearing

4 December 1985

Overview on Technical Counterintelligence and Security

Introduction

Mr. Chairman, I appear here today as the Administration representative to make a brief statement on the scope of the topic, talk about management and coordination, give a general description of some of the authorities for working in this area, and provide a perspective on resources. [redacted] 25X1

This is the fourth in your current series of hearings on counterintelligence and security and the comments today should be

considered as an extension and an elaboration of views previously presented in this series. [redacted] 25X1

In his statement on 1 November, the DCI noted the increased cooperation among CIA, NSA, and the State Department on providing greater security to our embassies, an area where technology-based collection efforts of the Soviets have been heavily concentrated. We are improving our understanding of our vulnerabilities and the strengths of the adversary. [redacted] 25X1 Soviets are further ahead in the clever application of technology than we thought and we must redress the balance. [redacted] 25X1

The DCI also noted the damage done by recent espionage cases. The assessments of these cases are yet to be completed, but they clearly demonstrate that man is the weak link, and that the most effective way to break through an adversary's technical defenses continues to be through human penetrations. [redacted] 25X1

Scope

This hearing is entitled technical counterintelligence and security, not a term widely used in the Intelligence Community. At your request, however, individual department and agency speakers will deal with security measures to counter Soviet and other hostile

technical threats to our communications, personnel, information systems, installations, and equipment. [redacted] 25X1

The opposition intelligence services--especially the KGB--clearly place a high priority on the use of technology to aid in their collection efforts. Our defensive measures have been stimulated [redacted] 25X1 by the scope of the Soviet effort [redacted] in the use of 25X1 technology-based collection activities. [redacted] 25X1

Our countermeasures against the hostile technical threats include the full range of counterintelligence and security disciplines:

-- countering the human collection threat;

-- surveillance and countersurveillance (e.g., secure radios);

-- physical security (including countering technical penetration of facilities);

-- technical surveillance countermeasures (i.e., prevention of bugging, telephone system exploitation, etc.);

-- communications security (COMSEC) (e.g., crypto machines and secure telephones);

-- emission security (TEMPEST) (e.g., shielded rooms and equipment);

-- computer security (COMPUSEC) (similar to COMSEC and TEMPEST, with focus on multi-level classification accesses);

-- information security (e.g., better access to, and handling/storage of, classified information);

-- personnel security (e.g., enhanced use of polygraphs, and investigations/reinvestigations);

-- industrial security (rigorous adherence to full spectrum of security requirements). [redacted] 25X1

Our highest priority has been for communications security, but more recently we have received priority surge-funding for technical surveillance countermeasures. Increased emphasis upon COMSEC, however, may well produce little increase in the security of communications if we do not also improve our personnel security systems. Technical improvement in the security of information processing and storage equipment in our embassies may be negated if we leave that equipment

exposed to foreign nationals inside the embassies or in support facilities. Our expensive, technical security measures must be accompanied by a full range of appropriate personnel investigations and physical security systems. 25X1

Management and Coordination

I note from your letter to the DCI on this hearing that you continue to be concerned about "the need for a comprehensive and integrated security program, with a permanent structure for planning and analysis to protect information and activities that have the greatest strategic importance"; and that you indicate your awareness "of recurrent proposals for a government-wide systems security budget." 25X1

In his overview comments at your first session on 1 November, the DCI discussed the Administration's principal organization for developing national counterintelligence and countermeasures policies and decisions. 25X1

I do not want to repeat all that the SIG-I and its two IGs do--one for counterintelligence and one for countermeasures--and the related roles of various top committees and councils such as the

Intelligence Research and Development Council (the IR&DC), the National Telecommunications and Information Systems Security Committee, the DCI's Security Committee and his Information Handling Committee. What I would like to stress is that overarching policy and strategy is developed and enunciated pragmatically by the IGs and SIG-I. Strategy and policy for each security discipline, e.g., COMSEC, is produced by committee/council structures tailored to the needs of the security community for that discipline. Use of "executive agents" and "lead agencies" that vary with the security discipline involved is a further manifestation of an avoidance of unnecessary and unwieldy layering. 25X1

Central management of security resources has no Community support. Each department's or agency's security program, of necessity, is adapted to its operational and programmatic needs. Indeed, central resource management could be detrimental. The IGs and the SIG-I, in their required periodic evaluation of the effectiveness of US counterintelligence and countermeasures against hostile intelligence threats, can and do provide guidance with respect to desired changes in the overall level of resources required to meet changing conditions. 25X1

The system we have does provide coordinated policy and resource guidance. It may need jacking up from time to time, as is true of any bureaucratic system. But, it works and is generally effective. 25X1

Let me now discuss the authorities for many of the security disciplines separately. [redacted] 25X1

Authorities

COMSEC--In October 1952 President Truman issued a classified directive that established the National Security Agency as well as the US Communications Security Board, and gave the responsibility for COMSEC to the NSA. President Carter's national security advisor, Dr. Brzezinski, signed a Presidential Directive (PD/NSC-24) in November 1977 to establish a new Telecommunications Protection Policy. Two years later, in June 1979, Defense Secretary Brown, as the Executive Agent for COMSEC, issued a National Communications Security Directive that set up the National Communications Security Committee (NCSC), the precursor to the National Telecommunications and Information Systems Security Committee (NTISSC), which dates from September 1984 with the signing by President Reagan of National Security Decision Directive 145, "National Policy on Telecommunications and Automated Information Systems Security." [redacted] 25X1

Additionally, in November 1983, NSDD-113 was signed by the President. It involves protection of communications systems used by key government officials in the Washington, D.C. area. This directive

was triggered by the collection and exploitation efforts of the Soviets and their Bloc surrogates, especially with regard to mobile communications. [redacted] 25X1

TEMPEST deals with the phenomenon of compromising emanations that was first recognized in the 1940s. It was the subject of policy directives in 1957 and 1963, but it was only in 1976, with the issuance of US COMSEC BOARD (USCSB) Policy 11-76, that NSA formally was assigned responsibility as manager of the nation's TEMPEST security program. The USCSB was replaced by the NCSC, and the NCSC by the NTISSC, but NSA continues to manage this program. Current national policy in the field of TEMPEST is contained in NCSC Policy No. 4, dated 16 January 1981, and will remain in effect until cancelled or modified by the NTISSC. [redacted] 25X1

COMPUSEC—The DoD Computer Security Center was established at NSA in January 1981 in response to DoD Directive 5215.1. Under NSDD-145 that center became the National Computer Security Center, and the Director of NSA became the National Manager for Telecommunications and Automated Information Systems Security. He operates under the guidance of an executive-level Steering Group, chaired by the Assistant to the President for National Security Affairs and including the Secretaries of State, Defense, and Treasury; the Attorney General; the Director of OMB; and the DCI. The three-pronged program of the center is directed toward:

a. improving the security of existing systems;

b. encouraging industry to develop new and better computer security products; and

c. undertaking and sponsoring research to improve the state of knowledge about computer security. 25X1

COMSEC, TEMPEST, and COMPUSEC: NSDD-145--As the DCI and the Director, NSA noted on 1 November, NSDD-145 makes substantial improvements in the administration's policy and organizational structure with regard to COMSEC, COMPUSEC, and emission security. It continues to provide a policy for the national security sector, and adds a policy on security for the civil elements of the government as well. Moreover, it recognizes that protection of our automated information and telecommunications systems are not just the concerns of government agencies, but are important to the private sector as well. It recognizes that large quantities of government and defense industry communications and information, which individually and in isolation may be unclassified, in the aggregate can reveal classified and other sensitive information. We know the Soviet 25X1 Bloc collects large quantities of "unclassified" information and communications. We also know that they have successfully and

effectively sorted such bulk information for the important intelligence elements contained therein. 25X1

TSCM--NSDD-145 cites the DCI as executive agent of technical surveillance countermeasures for detecting, neutralizing, or preventing hostile technical penetrations. Director of Central Intelligence Directive (DCID) 1/22, establishes policy and procedures for the conduct and coordination of TSCM. 25X1

25X1

I wish to place into the record as part of my statement a publication 25X1

This document lists finds, hazards, and other technical security anomalies submitted for analysis during this period. I believe the 23 finds--a substantial number of successful detections--reflect a reasonably healthy and active TSCM program. 25X1

Physical Security standards for SCI facilities have been set by NFIB/NFIC 9.1/47 as a result of the leadership of the DCI and his Security Committee in the SCI field. The National Security Act, 1947, as amended, implies authority to impose physical security requirements for information that reveals intelligence sources and methods. E.O. 12333, "United States Intelligence Activities," 4 December 1981, calls for protection of the security of installations, activities, information, property, and employees of various agencies. And it assigns to the DCI the responsibility to ensure the establishment by the Intelligence Community of common security and access standards for managing and handling foreign intelligence systems, information, or products and to ensure the programs are developed that protect intelligence sources, methods, and analytical procedures. [redacted] 25X1

The legal authority to impose physical security measures for those departments and agencies not concerned with SCI matters is implied in the authority of their heads to protect the operations and property of their respective organizations. In some instances, however, policy for physical protection and security is recognized or compelled by law or Executive order. For example, Title 18 USC, Sections 8422 and 1382, imposes criminal penalties for violations of the "Physical Security of Sensitive Conventional Arms...," and "Security of Military Installations and Resources." E.O. 12356, "National Security Information," 2 April 1982, and Information Security

Oversight Office Directive No. 1, 25 June 1982, provide safeguarding policy for the protection of classified information. And, Atomic Energy Act, 1954, Section 143 implies authority to impose specific physical security requirements for Restricted Data. [redacted] 25X1

Overflight Security--In October 1983 the President signed NSDD-107 to improve security from the technical-collection threat posed by hostile-country diplomatic and commercial aircraft that overfly the United States. The Overflight Security Committee established under this directive has been active in identifying flight routes to minimize the threat, and in establishing procedures for notification of pending overflight for sensitive government and military installations. The committee has also served an advisory role to the Department of State as it discusses bilateral commercial-aircraft agreements with Soviet Bloc countries. [redacted] 25X1

Countermeasures Resources--A Macro View

I have been talking up to now about scope, management, and coordination, and policy authorities to provide you with a broad insight into the scope of the technical counterintelligence and security problem. To round out this picture and underline its importance, I would like to give you some very rough estimates of the

size of the resources involved in the various security disciplines, and to discuss in brief how they are managed. 25X1

These estimates based largely on 1983 data are intended to be only a macro view. Security functions are decentralized management responsibilities funded by unlike program elements in different budgets. A precise tabulation of expenditures is unavailable. Therefore the figures that are available are quite soft, greatly limiting their utility for budget analysis. 25X1

The amounts of money expended by the nation on countermeasures 25X1

25X1

Almost all of these resources are outside the National Foreign Intelligence Program, and are not centrally managed. 25X1

25X1

The three big-ticket security disciplines are:

-- Industrial Security 25X1

-- Physical Security 25X1

-- Communications Security 25X1

Security disciplines with much lower expenditures, [redacted] 25X1

[redacted] include: 25X1

-- Emission Security;

-- Computer Security;

-- Personnel Security; and

-- Information Security.

[redacted] 25X1

The IG/CM and the SIG-I have been reviewing the general countermeasures-resources situation since early this year. Accordingly, the heads of the appropriate departments and agencies involved have been asked to review their respective resource management systems and procedures for countermeasures, especially where large sums are involved, with the objective of determining whether modifications to their countermeasures programs are indicated. The DCI intends to have a SIG-I review with department and agency managers later on. [redacted] 25X1

Two tentative conclusions may already be drawn, however.

-- The importance of personnel security, when viewed against the background of recent espionage disclosures and in the context of the total countermeasures-resource spectrum, would seem to require greater funding support, including for behavioral-science research leading to new ways of detecting problems with employees, and for developing better ways of conducting background investigations.

25X1

-- Funding for TSCM, given the seriousness of the hostile technical threat to us, has been insufficient and is now being increased. Nevertheless, there is much more that needs to be done, which will require a further growth in funding by an order of magnitude.

25X1

You have recently received a copy of the TSCM plan required supplemental appropriation. Those who will be testifying next regarding CIA, DoD, NSA, and State will be prepared to respond to any questions you may have concerning the plan.

25X1

25X1

Conclusion

The testimony today will provide you useful insight into the many programs designed to protect against hostile technical-intelligence threats to US communications, information systems, equipment and facilities--both at home and abroad--but especially abroad. I suggest that we begin with the Department of State representative, who will discuss the department's intentions for implementing Inman Panel recommendations on technical penetrations, and then proceed to hear from the CIA, NSA, and DoD representatives.

25X1